Claims

1. A multimedia contents protecting system for preventing multimedia contents, which are sent to an application program running on a client system, from leaking without permission through the use of an information providing system and the client system, the information providing system and the client system each having a Central Processing Unit (CPU), a volatile storage (memory), a non-volatile storage (hard disk) and an input/output device (keyboard, monitor, etc.), and being connected to each other through wired or wireless internal communication means or means for communicating with an external network, comprising:

the information providing system comprising,

encryption means (110) for encrypting original contents using one or more encryption keys and generating a content package (121),

provision means (120) for holding the encrypted content package (121) and providing the encrypted content package (121) to users on line, and

a Digital Rights Management (DRM) server (130) for managing generation of the encryption keys and performing various authentication operations; and

the client system comprising,

filtering means positioned between the application program and a device driver on a lower layer for hooking and converting a messages and a data packet, decrypting an encrypted data packet and sending the decrypted data packet to the application program,

control means for starting and terminating the application program and controlling the filtering means, and

an application program (144) for receiving the contents from the filtering means and playing the contents.

2. The multimedia contents protecting system as set forth in claim 1, wherein the encryption means (110) is a content packager (112) that receives the encryption keys generated by the DRM server (130) and encrypts the contents.

3. The multimedia contents protecting system as set forth in claim 1, wherein the provision means (120) is a content server (122) to which the content package (121) encrypted by the encryption means (110) is uploaded, and the content server (122) is a streaming server (122a) that provides actual streaming, a Web server (122b) that allows encrypted contents to be selected or provides download service, or a File Transfer Protocol (FTP) server.

4. The multimedia contents protecting system as set forth in claim 1, wherein the DRM server (130) comprises:

a DRM server DataBase (DB) (131) for storing various content information of the DRM server (130), the encryption keys, user information and application program information;

a DRM server component (132) for managing generation of the encryption keys and issuance of licenses;

a DRM license issuer (133) for issuing an encrypted license package in response to a request of the DRM controller (141); and

a DRM administrator (134) for performing various setting and administration.

5. The multimedia contents protecting system as set forth in claim 1, further comprising connecting means for enabling a connection to a billing server (150) or payment gateway server (160) to bill users for pay services.

6. The multimedia contents protecting system as set forth in claim 1, wherein the filtering means performs a filtering operation in kernel mode in response to an instruction of the control means, and is a network filter driver (404), or file filter driver (407) that converts and restores a file offset and a file length message requested by the application program (144) from the file system (405).

7. The multimedia contents protecting system as set forth in claim 1,

wherein the control means is a DRM controller (141) that is automatically activated to initiate the application program (144) when a user selects contents in a Web page in the case of a streaming manner or issues a command to open contents downloaded to a hard disk in the case of a downloading manner, accesses the DRM server (130), allows the contents and the user to be authenticated and receives the license package (143) including one or more decryption keys, terminates the filtering operation depending on terminating of the application program (144), and controls the filtering means.

8. The multimedia contents protecting system as set forth in claim 1, wherein the application program (144) is not a dedicated viewer program having a function of decrypting the content package, but a general application program capable of playing contents of a content package form.

9. The multimedia contents protecting system as set forth in claim 6, wherein the client system further comprises storage means that revises or edits contents that the application program (144) have decrypted and read, and encrypts and stores the revised or edited contents, and the network filter driver (404) or file filter driver (407) further comprises an encryption means.

10. The multimedia contents protecting system as set forth in claim 6, wherein the network filter driver (404) or file filter driver (407) is situated on an uppermost one of device driver layers in a direction toward the application program (144).

11. The multimedia contents protecting system as set forth in claim 10, wherein the network filter driver (404) uses a Transmission Control Protocol (TCP), or User Diagram Protocol (UDP) additionally having a function of correcting received data.

12. The multimedia contents protecting system as set forth in any of claims

1 to 11, wherein continuous content packets are sent and played in the case of a streaming manner, further comprising storage means for allowing content packets to be downloaded to the client system (140) and to be stored therein.

13. The multimedia contents protecting system as set forth in any of claims 1 to 12, wherein the multimedia contents are sent in one of a Video On Demand (VOD) streaming manner, a real-time live streaming manner, a complete downloading manner and a Hyper Text Transfer Protocol (HTTP) manner, or off line in a storage medium, such as Compact Disk (CD) or Digital Versatile Disk (DVD).

14. The multimedia contents protecting system as set forth in claim 13, further comprising a network filter driver disposed upstream of a network driver of an encoding system for performing hooking and encryption before the real-time live contents are sent to an external streaming server in the case of a real-time live streaming manner in which the sending of the multimedia contents are performed through a multimedia receiving device and the encoding system.

15. The multimedia contents protecting system as set forth in claim 1, wherein the encrypted content package (142) comprises at least a data object portion that are encrypted contents (142a) and a header object portion that are non-encrypted meta data (142b).

16. The multimedia contents protecting system as set forth in claim 15, wherein a DRM package header of the encrypted content package (142) is recorded in the header object of a multimedia content file form.

17. The multimedia contents protecting system as set forth in claim 16, wherein the DRM package header includes a version number, a content Uniform Resource Identifier (URI) length, a content type length, a content URI, a content type, a header length, a data length, an encryption method, a rights issuer Uniform

Resource Identifier (URL), a content name, a content description, a content vendor, an icon URI, a digital signature, and a content server URL.

18. The multimedia contents protecting system as set forth in claim 15, wherein the data object that is the encrypted contents (142a) is fully encrypted or partially encrypted in one or more predetermined frames.

19. The multimedia contents protecting system as set forth in claim 15, wherein the client system further comprises storage means for storing the encrypted content package.

20. The multimedia contents protecting system as set forth in claim 1, wherein the encrypted license package (143) sent to the client system in response to a request of the user for authentication comprises:

a decryption key (143a) for performing decryption; and

usage rights (143b) including at least a count of use and a period of use of the contents and terminal restriction information.

21. A multimedia contents protecting method of preventing multimedia contents, which are sent to an application program running on a client system, from leaking without permission through the use of an information providing system and the client system, the information providing system and the client system each having a CPU, a volatile storage (memory), a non-volatile storage (hard disk) and an input/output device (keyboard, monitor, etc.), and being connected to each other through wired or wireless internal communication means or means for communicating with an external network, comprising:

the encrypting and uploading step of converting original contents (111) into an encrypted content package (121) using one or more encryption keys of a DRM server and uploading the encrypted content package (121) to a content server (122);

the initiating and connecting step of connecting the client system to the

content server (122) and initiating streaming or downloading service by selecting contents in a Web server (122b) or FTP server;

the decrypting and playing step of decrypting and playing content data through an application program (144) in response to a signal from a player during sending in the case of a streaming manner, or after downloading in the case of a downloading manner; and

the terminating step of terminating an operation of the application program (144) and a filtering operation and disconnecting the client system from the content server (122) in the case of a streaming manner when a DRM controller (141) detects a termination command of the application program (144).

22. The multimedia contents protecting method as set forth in claim 21, wherein the encrypting and uploading step comprises:

the step (S21 and S22) of the content packager (112) requesting and obtaining an authentication from the DRM server (130);

the step (S23 and S24) of the content packager (112) requesting and obtaining one or more encryption keys from the DRM server (130);

the step of the content packager (112) encrypting contents using the encryption keys;

the step (S25 and S26) of the content packager (112) requesting and obtaining an authentication from the content server (122); and

the step (S27) of the content packager (112) sending the encrypted content package (121) to the content server (122).

23. The multimedia contents protecting method as set forth in claim 21, wherein the initiating and connecting step comprises:

the step (S31) of the Web server (122b) or FTP server sending content identification information and user identification information to the DRM controller (141) if the application program (144) is commanded to retrieve contents after downloading of the contents in the case of a downloading manner, or if contents are selected on a Web page in the case of a streaming manner;

the step (S32 and S33) of the DRM controller (141) requesting content and user authentication from the DRM server (130) and receiving license authentication including a decryption key and user authority information;

the step (S34) of the DRM controller (141) sending to the application program (144) an URL of the content server (122) in the case of a streaming manner, a position of a hard disk where the contents are stored in the case of a complete downloading manner, and both the URL of the content server (122) and the position of the hard disk in the case of a HTTP streaming manner, after initiating the application program (144); and

the step (S35) of the DRM controller (141) requesting content data from the content server (122) in the case of a streaming manner, from the file system in the case of a downloading manner, and from both the content server (122) and the file system in the case of a HTTP streaming manner.

24. The multimedia contents protecting method as set forth in claim 23, further comprising:

the connection preparing step of performing examination of a handler and registration of a process after the application program (144) is initiated; and

the connecting step of performing next registration of a process and ascertainment and storing of a remote port.

25. The multimedia contents protecting method as set forth in claim 24, wherein the connection preparing step comprises:

the step of starting and temporarily stopping the application program (144);

the step of the DRM controller (141) determining whether the handler is zero by hooking a message between the application program (144) and the network driver or file system using filtering means;

the step of deleting an address handle to cancel the connection and sending a message to the network driver or file system if the handler is zero, and determining whether a process is registered in the filtering means if the handler is not zero;

the step of sending a message to the network driver or file system if the process is not registered in the filtering means, and registering an address handle, setting a my event handler, storing a local port and sending a changed message to the network driver or file system if the process is registered in the filtering means; and

the step of the application program (144) receiving a ready message from the network driver or file system through the sending of the message.

26. The multimedia contents protecting method as set forth in claim 24, wherein the connecting step comprises:

the step of the filtering means hooking a message between the application program (144) and the network driver or file system and determining whether the process is registered in the filtering means;

the step of sending the message the network driver or file system if the process is not registered in the filtering means, and determining whether a remote port has a predetermined number if the process is registered in the filtering means; and

the step of sending the message to the network driver or file system if the remote port does not have the predetermined number, and sending the message to the network driver or file system after storing a remote port number in an address handle structure having a local port connected to the remote port if the remote port has the predetermined number.

27. The multimedia contents protecting method as set forth in claim 21, wherein the encrypting and playing step comprises:

the step (901) of a storage in the case of downloading, and the content server (122) in the case of streaming periodically sending a data packet to the application program (144), along with control information;

the step (403) of hooking the data packet using the filtering means;

the step (902) of determining whether a remote port has a predetermined number in a state in which the my event handler is activated;

the step of sending the data packet to the application program (144) if the remote port does not have the predetermined number, and decrypting the data packet and sending the decrypted data packet to the application program (144) if the remote port has the predetermined number; and

the step of playing the data packet by repeating the above steps.

28. The multimedia contents protecting method as set forth in claim 27, further comprising:

the step of determining whether the data packet is stored in the hard disk before being decrypted (905); and

the step of decrypting the data packet if the data packet is not stored in the hard disk, and decrypting the data packet after being stored in the hard disk if the data packet is not stored in the hard disk.

29. The multimedia contents protecting method as set forth in claim 21, wherein the terminating step comprises:

the step of the DRM controller (141) detecting a termination message of the application program (144) every cycle in which the content data packet is decrypted and played; and

the step of returning to the decrypting and playing step if the termination message is not detected, and disconnecting the client system from the content server (122) or hard disk by terminating the application program (144) and deleting the address handle if the termination message is detected.

30. A computer-readable storage medium for storing a multimedia contents protecting method of preventing multimedia contents, which are sent to an application program running on a client system, from leaking without permission through the use of an information providing system and the client system, the information providing system and the client system each having a CPU, a volatile storage (memory), a non-volatile storage (hard disk) and an input/output device (keyboard, monitor, etc.), and being connected to each other through wired or

wireless internal communication means or means for communicating with an external network, the multimedia contents protecting method comprising:

the encrypting and uploading step of converting original contents (111) into an encrypted content package (121) using one or more encryption keys of a DRM server and uploading the encrypted content package (121) to a content server (122);

the initiating and connecting step of connecting the client system to the content server (122) and initiating streaming or downloading service by a user selecting contents in a Web server (122b) or FTP server;

the decrypting and playing step of decrypting and playing content data through an application program (144) in response to a signal from a player during sending in the case of a streaming manner, or after downloading in the case of a downloading manner; and

the terminating step of terminating an operation of the application program (144) and a filtering operation and disconnecting the client system from the content server (122) in the case of a streaming manner when a DRM controller (141) detects a termination command of the application program (144).